SEC. 4497. CERTIFICATIONS REGARDING ACCESS TO EXPORT CONTROLLED TECHNOLOGY IN EDUCATIONAL AND CULTURAL EXCHANGE PROGRAMS.

Section 102(b)(5) of the Mutual Educational and Cultural Exchange Act of 1961 (22 U.S.C. 2452(b)(5)) is amended to read as follows:

''(5) promoting and supporting medical, scientific, cultural, and educational research and development by developing exchange programs for foreign researchers and scientists, while protecting technologies regulated by export control laws important to the national security and economic interests of the United States, by requiring—

''(A) the sponsor to certify to the Department of State that the sponsor, after reviewing all regulations related to the Export Controls Act of 2018 (50 U.S.C. 4811 et seq.) and the Arms Export Control Act (22 U.S.C. 2751 et seq.), has determined that—

''(i) a license is not required from the Department of Commerce or the Department of State to release such technology or technical data to the exchange visitor; or

''(ii)(I) a license is required from the Department of Commerce or the Department of State to release such technology or technical data to the exchange visitor; and

''(II) the sponsor will prevent access to the controlled technology or technical data by the exchange visitor until the sponsor—

''(aa) has received the required license or other authorization to release it to the visitor; and

''(bb) has provided a copy of such license or authorization to the Department of State; and

''(B) if the sponsor maintains export controlled technology or technical data, the sponsor to submit to the Department of State the sponsor's plan to prevent unauthorized export or transfer of any controlled items, materials, information, or technology at the sponsor organization or entities associated with a sponsor's administration of the exchange visitor program.''.

SEC. 4498. PRIVACY AND CONFIDENTIALITY.

Nothing in this subtitle may be construed as affecting the rights and requirements provided in section 552a of title 5, United States Code (commonly known as the ''Privacy Act of 1974'') or subchapter III of chapter 35 of title 44, United States Code (commonly known as the ''Confidential Information Protection and Statistical Efficiency Act of 2018'').

SA 4292. Mr. PORTMAN submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

DIVISION E—SECURING AMERICA'S FUTURE

SEC. 4001. SHORT TITLE; TABLE OF CONTENTS.

This division may be cited as the ''Securing America's Future Act''.

TITLE I—ADVANCING AMERICAN AI

SEC. 4201. SHORT TITLE.

This subtitle may be cited as the ''Advancing American AI Act''.

SEC. 4202. PURPOSE.

The purposes of this subtitle are to—

(1) encourage agency artificial intelligence-related programs and initiatives that enhance the competitiveness of the United States and foster an approach to artificial intelligence that builds on the strengths of the United States in innovation and entrepreneurialism;

(2) enhance the ability of the Federal Government to translate research advances into artificial intelligence applications to modernize systems and assist agency leaders in fulfilling their missions;

(3) promote adoption of modernized business practices and advanced technologies across the Federal Government that align with the values of the United States, including the protection of privacy, civil rights, and civil liberties; and

(4) test and harness applied artificial intelligence to enhance mission effectiveness and business practice efficiency.

SEC. 4203. DEFINITIONS.

In this subtitle:

(1) AGENCY.—The term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code.

(2) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) the Committee on Oversight and Reform of the House of Representatives.

(3) ARTIFICIAL INTELLIGENCE.—The term ''artificial intelligence'' has the meaning given the term in section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (10 U.S.C. 2358 note).

(4) ARTIFICIAL INTELLIGENCE SYSTEM.—The term ''artificial intelligence system''—

(A) means any data system, software, application, tool, or utility that operates in whole or in part using dynamic or static machine learning algorithms or other forms of artificial intelligence, whether—

(i) the data system, software, application, tool, or utility is established primarily for the purpose of researching, developing, or implementing artificial intelligence technology; or

(ii) artificial intelligence capability is integrated into another system or agency business process, operational activity, or technology system; and

(B) does not include any common commercial product within which artificial intelligence is embedded, such as a word processor or map navigation system.

(5) DEPARTMENT.—The term ''Department'' means the Department of Homeland Security.

(6) DIRECTOR.—The term ''Director'' means the Director of the Office of Management and Budget.

SEC. 4204. PRINCIPLES AND POLICIES FOR USE OF ARTIFICIAL INTELLIGENCE IN GOVERNMENT.

(a) GUIDANCE.—The Director shall, when developing the guidance required under section 104(a) of the AI in Government Act of 2020 (title I of division U of Public Law 116–260), consider—

(1) the considerations and recommended practices identified by the National Security Commission on Artificial Intelligence in the report entitled ''Key Considerations for the Responsible Development and Fielding of AI'', as updated in April 2021;

(2) the principles articulated in Executive Order 13960 (85 Fed. Reg. 78939; relating to promoting the use of trustworthy artificial intelligence in Government); and

(3) the input of—

(A) the Privacy and Civil Liberties Oversight Board;

(B) relevant interagency councils, such as the Federal Privacy Council, the Chief Information Officers Council, and the Chief Data Officers Council;

(C) other governmental and nongovernmental privacy, civil rights, and civil liberties experts; and

(D) any other individual or entity the Director determines to be appropriate.

(b) DEPARTMENT POLICIES AND PROCESSES FOR PROCUREMENT AND USE OF ARTIFICIAL INTELLIGENCE-ENABLED SYSTEMS.—Not later than 180 days after the date of enactment of this Act—

(1) the Secretary of Homeland Security, with the participation of the Chief Procurement Officer, the Chief Information Officer, the Chief Privacy Officer, and the Officer for Civil Rights and Civil Liberties of the Department and any other person determined to be relevant by the Secretary of Homeland Security, shall issue policies and procedures for the Department related to—

(A) the acquisition and use of artificial intelligence; and

(B) considerations for the risks and impacts related to artificial intelligence-enabled systems, including associated data of machine learning systems, to ensure that full consideration is given to—

(i) the privacy, civil rights, and civil liberties impacts of artificial intelligence-enabled systems; and

(ii) security against misuse, degradation, or rending inoperable of artificial intelligence-enabled systems; and

(2) the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department shall report to Congress on any additional staffing or funding resources that may be required to carry out the requirements of this subsection.

(c) INSPECTOR GENERAL.—Not later than 180 days after the date of enactment of this Act, the Inspector General of the Department shall identify any training and investments needed to enable employees of the Office of the Inspector General to continually advance their understanding of—

(1) artificial intelligence systems;

(2) best practices for governance, oversight, and audits of the use of artificial intelligence systems; and

(3) how the Office of the Inspector General is using artificial intelligence to enhance audit and investigative capabilities, including actions to—

(A) ensure the integrity of audit and investigative results; and

(B) guard against bias in the selection and conduct of audits and investigations.

(d) ARTIFICIAL INTELLIGENCE HYGIENE AND PROTECTION OF GOVERNMENT INFORMATION, PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES.—

(1) ESTABLISHMENT.—Not later than 1 year after the date of enactment of this Act, the Director, in consultation with a working group consisting of members selected by the Director from appropriate interagency councils, shall develop an initial means by which to—

(A) ensure that contracts for the acquisition of an artificial intelligence system or service—

(i) align with the guidance issued to the head of each agency under section 104(a) of the AI in Government Act of 2020 (title I of division U of Public Law 116–260);

(ii) address protection of privacy, civil rights, and civil liberties;

(iii) address the ownership and security of data and other information created, used, processed, stored, maintained, disseminated, disclosed, or disposed of by a contractor or subcontractor on behalf of the Federal Government; and

(iv) include considerations for securing the training data, algorithms, and other components of any artificial intelligence system against misuse, unauthorized alteration, degradation, or rendering inoperable; and

(B) address any other issue or concern determined to be relevant by the Director to ensure appropriate use and protection of privacy and Government data and other information.

(2) CONSULTATION.—In developing the considerations under paragraph (1)(A)(iv), the Director shall consult with the Secretary of Homeland Security, the Director of the National Institute of Standards and Technology, and the Director of National Intelligence.

(3) REVIEW.—The Director—

(A) should continuously update the means developed under paragraph (1); and

(B) not later than 2 years after the date of enactment of this Act and not less frequently than every 2 years thereafter, shall update the means developed under paragraph (1).

(4) BRIEFING.—The Director shall brief the appropriate congressional committees—

(A) not later than 90 days after the date of enactment of this Act and thereafter on a quarterly basis until the Director first implements the means developed under paragraph (1); and

(B) annually thereafter on the implementation of this subsection.

(5) SUNSET.—This subsection shall cease to be effective on the date that is 5 years after the date of enactment of this Act.

SEC. 4205. AGENCY INVENTORIES AND ARTIFICIAL INTELLIGENCE USE CASES.

(a) INVENTORY.—Not later than 60 days after the date of enactment of this Act, and continuously thereafter for a period of 5 years, the Director, in consultation with the Chief Information Officers Council, the Chief Data Officers Council, and other interagency bodies as determined to be appropriate by the Director, shall require the head of each agency to—

(1) prepare and maintain an inventory of the artificial intelligence use cases of the agency, including current and planned uses;

(2) share agency inventories with other agencies, to the extent practicable and consistent with applicable law and policy, including those concerning protection of privacy and of sensitive law enforcement, national security, and other protected information; and

(3) make agency inventories available to the public, in a manner determined by the Director, and to the extent practicable and in accordance with applicable law and policy, including those concerning the protection of privacy and of sensitive law enforcement, national security, and other protected information.

(b) CENTRAL INVENTORY.—The Director is encouraged to designate a host entity and ensure the creation and maintenance of an online public directory to—

(1) make agency artificial intelligence use case information available to the public and those wishing to do business with the Federal Government; and

(2) identify common use cases across agencies.

(c) SHARING.—The sharing of agency inventories described in subsection (a)(2) may be coordinated through the Chief Information Officers Council, the Chief Data Officers Council, the Chief Financial Officers Council, the Chief Acquisition Officers Council, or other interagency bodies to improve interagency coordination and information sharing for common use cases.

SEC. 4206. RAPID PILOT, DEPLOYMENT AND SCALE OF APPLIED ARTIFICIAL INTELLIGENCE CAPABILITIES TO DEMONSTRATE MODERNIZATION ACTIVITIES RELATED TO USE CASES.

(a) IDENTIFICATION OF USE CASES.—Not later than 270 days after the date of enactment of this Act, the Director, in consultation with the Chief Information Officers Council, the Chief Data Officers Council, and other interagency bodies as determined to be appropriate by the Director, shall identify 4 new use cases for the application of artificial intelligence-enabled systems to support interagency or intra-agency modernization initiatives that require linking multiple siloed internal and external data sources, consistent with applicable laws and policies, including those relating to the protection of privacy and of sensitive law enforcement, national security, and other protected information.

(b) PILOT PROGRAM.—

(1) PURPOSES.—The purposes of the pilot program under this subsection include—

(A) to enable agencies to operate across organizational boundaries, coordinating between existing established programs and silos to improve delivery of the agency mission; and

(B) to demonstrate the circumstances under which artificial intelligence can be used to modernize or assist in modernizing legacy agency systems.

(2) DEPLOYMENT AND PILOT.—Not later than 1 year after the date of enactment of this Act, the Director, in coordination with the heads of relevant agencies and other officials as the Director determines to be appropriate, shall ensure the initiation of the piloting of the 4 new artificial intelligence use case applications identified under subsection (a), leveraging commercially available technologies and systems to demonstrate scalable artificial intelligence-enabled capabilities to support the use cases identified under subsection (a).

(3) RISK EVALUATION AND MITIGATION PLAN.—In carrying out paragraph (2), the Director shall require the heads of agencies to—

(A) evaluate risks in utilizing artificial intelligence systems; and

(B) develop a risk mitigation plan to address those risks, including consideration of—

(i) the artificial intelligence system not performing as expected;

(ii) the lack of sufficient or quality training data; and

(iii) the vulnerability of a utilized artificial intelligence system to unauthorized manipulation or misuse.

(4) PRIORITIZATION.—In carrying out paragraph (2), the Director shall prioritize modernization projects that—

(A) would benefit from commercially available privacy-preserving techniques, such as use of differential privacy, federated learning, and secure multiparty computing; and

(B) otherwise take into account considerations of civil rights and civil liberties.

(5) USE CASE MODERNIZATION APPLICATION AREAS.—Use case modernization application areas described in paragraph (2) shall include not less than 1 from each of the following categories:

(A) Applied artificial intelligence to drive agency productivity efficiencies in predictive supply chain and logistics, such as—

(i) predictive food demand and optimized supply;

(ii) predictive medical supplies and equipment demand and optimized supply; or

(iii) predictive logistics to accelerate disaster preparedness, response, and recovery.

(B) Applied artificial intelligence to accelerate agency investment return and address mission-oriented challenges, such as—

(i) applied artificial intelligence portfolio management for agencies;

(ii) workforce development and upskilling;

(iii) redundant and laborious analyses;

(iv) determining compliance with Government requirements, such as with grants management; or

(v) outcomes measurement to measure economic and social benefits.

(6) REQUIREMENTS.—Not later than 3 years after the date of enactment of this Act, the Director, in coordination with the heads of relevant agencies and other officials as the Director determines to be appropriate, shall establish an artificial intelligence capability within each of the 4 use case pilots under this subsection that—

(A) solves data access and usability issues with automated technology and eliminates or minimizes the need for manual data cleansing and harmonization efforts;

(B) continuously and automatically ingests data and updates domain models in near real-time to help identify new patterns and predict trends, to the extent possible, to help agency personnel to make better decisions and take faster actions;

(C) organizes data for meaningful data visualization and analysis so the Government has predictive transparency for situational awareness to improve use case outcomes;

(D) is rapidly configurable to support multiple applications and automatically adapts to dynamic conditions and evolving use case requirements, to the extent possible;

(E) enables knowledge transfer and collaboration across agencies; and

(F) preserves intellectual property rights to the data and output for benefit of the Federal Government and agencies.

(c) BRIEFING.—Not earlier than 270 days but not later than 1 year after the date of enactment of this Act, and annually thereafter for 4 years, the Director shall brief the appropriate congressional committees on the activities carried out under this section and results of those activities.

(d) SUNSET.—The section shall cease to be effective on the date that is 5 years after the date of enactment of this Act.

SEC. 4207. ENABLING ENTREPRENEURS AND AGENCY MISSIONS.

(a) INNOVATIVE COMMERCIAL ITEMS.—Section 880 of the National Defense Authorization Act for Fiscal Year 2017 (41 U.S.C. 3301 note) is amended—

(1) in subsection (c), by striking ''$10,000,000'' and inserting ''$25,000,000'';

(2) by amending subsection (f) to read as follows:

''(f) DEFINITIONS.—In this section—

''(1) the term 'commercial product'—

''(A) has the meaning given the term 'commercial item' in section 2.101 of the Federal Acquisition Regulation; and

''(B) includes a commercial product or a commercial service, as defined in sections 103 and 103a, respectively, of title 41, United States Code; and

''(2) the term 'innovative' means—

''(A) any new technology, process, or method, including research and development; or

''(B) any new application of an existing technology, process, or method.''; and

(3) in subsection (g), by striking ''2022'' and insert ''2027''.

(b) DHS OTHER TRANSACTION AUTHORITY.—Section 831 of the Homeland Security Act of 2002 (6 U.S.C. 391) is amended—

(1) in subsection (a)—

(A) in the matter preceding paragraph (1), by striking ''September 30, 2017'' and inserting ''September 30, 2024''; and

(B) by amending paragraph (2) to read as follows:

''(2) PROTOTYPE PROJECTS.—The Secretary—

''(A) may, under the authority of paragraph (1), carry out prototype projects under section 2371b of title 10, United States Code; and

''(B) in applying the authorities of such section 2371b, the Secretary shall perform the functions of the Secretary of Defense as prescribed in such section.'';

(2) in subsection (c)(1), by striking ''September 30, 2017'' and inserting ''September 30, 2024''; and

(3) in subsection (d), by striking ''section 845(e)'' and all that follows and inserting ''section 2371b(e) of title 10, United States Code.''.

(c) COMMERCIAL OFF THE SHELF SUPPLY CHAIN RISK MANAGEMENT TOOLS.—The General Services Administration is encouraged to pilot commercial off the shelf supply chain risk management tools to improve the ability of the Federal Government to characterize, monitor, predict, and respond to specific supply chain threats and vulnerabilities that could inhibit future Federal acquisition operations.

TITLE II—PERSONNEL

Subtitle A—Facilitating Federal Employee Reskilling

SEC. 4301. SHORT TITLE.

This subtitle may be cited as the ''Facilitating Federal Employee Reskilling Act''.

SEC. 4302. RESKILLING FEDERAL EMPLOYEES.

(a) DEFINITIONS.—In this section:

(1) AGENCY.—The term ''agency'' has the meaning given the term ''Executive agency'' in section 105 of title 5, United States Code.

(2) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means—

(A) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) the Committee on Oversight and Reform of the House of Representatives.

(3) COMPETITIVE SERVICE.—The term ''competitive service'' has the meaning given the term in section 2102 of title 5, United States Code.

(4) DIRECTOR.—The term ''Director'' means the Director of the Office of Personnel Management.

(5) EMPLOYEE.—The term ''employee'' means an employee serving in a position in the competitive service or the excepted service.

(6) EXCEPTED SERVICE.—The term ''excepted service'' has the meaning given the term in section 2103 of title 5, United States Code.

(7) FEDERAL RESKILLING PROGRAM.—The term ''Federal reskilling program'' means a program established by the head of an agency or the Director to provide employees with the technical skill or expertise that would qualify the employees to serve in a different position in the competitive service or the excepted service that requires such technical skill or expertise.

(b) REQUIREMENTS.—With respect to a Federal reskilling program established by the head of an agency or by the Director before, on, or after the date of enactment of this Act, the agency head or the Director, as applicable, shall ensure that the Federal reskilling program—

(1) is implemented in a manner that is in accordance with the bar on prohibited personnel practices under section 2302 of title 5, United States Code, and consistent with the merit system principles under section 2301 of title 5, United States Code, including by using merit-based selection procedures for participation by employees in the Federal reskilling program;

(2) includes appropriate limitations or restrictions associated with implementing the Federal reskilling program, which shall be consistent with any regulations prescribed by the Director under subsection (e);

(3) provides that any new position to which an employee who participates in the Federal reskilling program is transferred will utilize the technical skill or expertise that the employee acquired by participating in the Federal reskilling program;

(4) includes the option for an employee participating in the Federal reskilling program to return to the original position of the employee, or a similar position, particularly if the employee is unsuccessful in the position to which the employee transfers after completing the Federal reskilling program;

(5) provides that an employee who successfully completes the Federal reskilling program and transfers to a position that requires the technical skill or expertise provided through the Federal reskilling program shall be entitled to have the grade of the position held immediately before the transfer in a manner in accordance with section 5362 of title 5, United States Code;

(6) provides that an employee serving in a position in the excepted service may not transfer to a position in the competitive service solely by reason of the completion of the Federal reskilling program by the employee; and

(7) includes a mechanism to track outcomes of the Federal reskilling program in accordance with the metrics established under subsection (c).

(c) REPORTING AND METRICS.—Not later than 1 year after the date of enactment of this Act, the Director shall establish reporting requirements for, and standardized metrics and procedures for agencies to track outcomes of, Federal reskilling programs, which shall include, with respect to each Federal reskilling program—

(1) providing a summary of the Federal reskilling program;

(2) collecting and reporting demographic and employment data with respect to employees who have applied for, participated in, or completed the Federal reskilling program;

(3) attrition of employees who have completed the Federal reskilling program; and

(4) any other measures or outcomes that the Director determines to be relevant.

(d) GAO REPORT.—Not later than 3 years after the date of enactment of this Act, the Comptroller General of the United States shall conduct a comprehensive study of, and submit to Congress a report on, Federal reskilling programs that includes—

(1) a summary of each Federal reskilling program and methods by which each Federal reskilling program recruits, selects, and retrains employees;

(2) an analysis of the accessibility of each Federal reskilling program for a diverse set of candidates;

(3) an evaluation of the effectiveness, costs, and benefits of the Federal reskilling programs; and

(4) recommendations to improve Federal reskilling programs to accomplish the goal of reskilling the Federal workforce.

(e) REGULATIONS.—The Director—

(1) not later than 1 year after the date of enactment of this Act, shall prescribe regulations for the reporting requirements and metrics and procedures under subsection (c);

(2) may prescribe additional regulations, as the Director determines necessary, to provide for requirements with respect to, and the implementation of, Federal reskilling programs; and

(3) with respect to any regulation prescribed under this subsection, shall brief the appropriate committees of Congress with respect to the regulation not later than 30 days before the date on which the final version of the regulation is published.

(f) RULE OF CONSTRUCTION.—Nothing in this section may be construed to require the head of an agency or the Director to establish a Federal reskilling program.

(g) USE OF FUNDS.—Any Federal reskilling program established by the head of an agency or the Director shall be carried out using amounts otherwise made available to that agency head or the Director, as applicable.

Subtitle B—Federal Rotational Cyber Workforce Program

SEC. 4351. SHORT TITLE.

This subtitle may be cited as the ''Federal Rotational Cyber Workforce Program Act of 2021''.

SEC. 4352. DEFINITIONS.

In this subtitle:

(1) AGENCY.—The term ''agency'' has the meaning given the term ''Executive agency'' in section 105 of title 5, United States Code, except that the term does not include the Government Accountability Office.

(2) COMPETITIVE SERVICE.—The term ''competitive service'' has the meaning given that term in section 2102 of title 5, United States Code.

(3) COUNCILS.—The term ''Councils'' means—

(A) the Chief Human Capital Officers Council established under section 1303 of the Chief Human Capital Officers Act of 2002 (5 U.S.C. 1401 note); and

(B) the Chief Information Officers Council established under section 3603 of title 44, United States Code.

(4) CYBER WORKFORCE POSITION.—The term ''cyber workforce position'' means a position identified as having information technology, cybersecurity, or other cyber-related functions under section 303 of the Federal Cybersecurity Workforce Assessment Act of 2015 (5 U.S.C. 301 note).

(5) DIRECTOR.—The term ''Director'' means the Director of the Office of Personnel Management.

(6) EMPLOYEE.—The term ''employee'' has the meaning given the term in section 2105 of title 5, United States Code.

(7) EMPLOYING AGENCY.—The term ''employing agency'' means the agency from which an employee is detailed to a rotational cyber workforce position.

(8) EXCEPTED SERVICE.—The term ''excepted service'' has the meaning given that term in section 2103 of title 5, United States Code.

(9) ROTATIONAL CYBER WORKFORCE POSITION.—The term ''rotational cyber workforce position'' means a cyber workforce position with respect to which a determination has been made under section 4353(a)(1).

(10) ROTATIONAL CYBER WORKFORCE PROGRAM.—The term ''rotational cyber workforce program'' means the program for the detail of employees among rotational cyber workforce positions at agencies.

(11) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security.

SEC. 4353. ROTATIONAL CYBER WORKFORCE POSITIONS.

(a) DETERMINATION WITH RESPECT TO ROTATIONAL SERVICE.—

(1) IN GENERAL.—The head of each agency may determine that a cyber workforce position in that agency is eligible for the rotational cyber workforce program, which shall not be construed to modify the requirement under section 4354(b)(3) that participation in the rotational cyber workforce program by an employee shall be voluntary.

(2) NOTICE PROVIDED.—The head of an agency shall submit to the Director—

(A) notice regarding any determination made by the head of the agency under paragraph (1); and

(B) for each position with respect to which the head of the agency makes a determination under paragraph (1), the information required under subsection (b)(1).

(b) PREPARATION OF LIST.—The Director, with assistance from the Councils and the Secretary, shall develop a list of rotational cyber workforce positions that—

(1) with respect to each such position, to the extent that the information does not disclose sensitive national security information, includes—

(A) the title of the position;
(B) the occupational series with respect to the position;
(C) the grade level or work level with respect to the position;
(D) the agency in which the position is located;
(E) the duty location with respect to the position; and
(F) the major duties and functions of the position; and
(2) shall be used to support the rotational cyber workforce program.
(c) DISTRIBUTION OF LIST.—Not less frequently than annually, the Director shall distribute an updated list developed under subsection (b) to the head of each agency and other appropriate entities.

SEC. 4354. ROTATIONAL CYBER WORKFORCE PROGRAM.

(a) OPERATION PLAN.—
(1) IN GENERAL.—Not later than 270 days after the date of enactment of this Act, and in consultation with the Councils, the Secretary, representatives of other agencies, and any other entity as the Director determines appropriate, the Director shall develop and issue a Federal Rotational Cyber Workforce Program operation plan providing policies, processes, and procedures for a program for the detailing of employees among rotational cyber workforce positions at agencies, which may be incorporated into and implemented through mechanisms in existence on the date of enactment of this Act.
(2) UPDATING.—The Director may, in consultation with the Councils, the Secretary, and other entities as the Director determines appropriate, periodically update the operation plan developed and issued under paragraph (1).
(b) REQUIREMENTS.—The operation plan developed and issued under subsection (a) shall, at a minimum—
(1) identify agencies for participation in the rotational cyber workforce program;
(2) establish procedures for the rotational cyber workforce program, including—
(A) any training, education, or career development requirements associated with participation in the rotational cyber workforce program;
(B) any prerequisites or requirements for participation in the rotational cyber workforce program; and
(C) appropriate rotational cyber workforce program performance measures, reporting requirements, employee exit surveys, and other accountability devices for the evaluation of the program;
(3) provide that participation in the rotational cyber workforce program by an employee shall be voluntary;
(4) provide that an employee shall be eligible to participate in the rotational cyber workforce program if the head of the employing agency of the employee, or a designee of the head of the employing agency of the employee, approves of the participation of the employee;
(5) provide that the detail of an employee to a rotational cyber workforce position under the rotational cyber workforce program shall be on a nonreimbursable basis;
(6) provide that agencies may agree to partner to ensure that the employing agency of an employee who participates in the rotational cyber workforce program is able to fill the position vacated by the employee;
(7) require that an employee detailed to a rotational cyber workforce position under the rotational cyber workforce program, upon the end of the period of service with respect to the detail, shall be entitled to return to the position held by the employee, or an equivalent position, in the employing agency of the employee without loss of pay, seniority, or other rights or benefits to which the employee would have been entitled had the employee not been detailed;
(8) provide that discretion with respect to the assignment of an employee under the rotational cyber workforce program shall remain with the employing agency of the employee;
(9) require that an employee detailed to a rotational cyber workforce position under the rotational cyber workforce program in an agency that is not the employing agency of the employee shall have all the rights that would be available to the employee if the employee were detailed under a provision of law other than this subtitle from the employing agency to the agency in which the rotational cyber workforce position is located;
(10) provide that participation by an employee in the rotational cyber workforce program shall not constitute a change in the conditions of the employment of the employee; and
(11) provide that an employee participating in the rotational cyber workforce program shall receive performance evaluations relating to service in the rotational cyber workforce program in a participating agency that are—
(A) prepared by an appropriate officer, supervisor, or management official of the employing agency, acting in coordination with the supervisor at the agency in which the employee is performing service in the rotational cyber workforce position;
(B) based on objectives identified in the operation plan with respect to the employee; and
(C) based in whole or in part on the contribution of the employee to the agency in which the employee performed such service, as communicated from that agency to the employing agency of the employee.
(c) PROGRAM REQUIREMENTS FOR ROTATIONAL SERVICE.—
(1) IN GENERAL.—An employee serving in a cyber workforce position in an agency may, with the approval of the head of the agency, submit an application for detail to a rotational cyber workforce position that appears on the list developed under section 4353(b).
(2) OPM APPROVAL FOR CERTAIN POSITIONS.—An employee serving in a position in the excepted service may only be selected for a rotational cyber workforce position that is in the competitive service with the prior approval of the Office of Personnel Management, in accordance with section 300.301 of title 5, Code of Federal Regulations, or any successor thereto.
(3) SELECTION AND TERM.—
(A) SELECTION.—The head of an agency shall select an employee for a rotational cyber workforce position under the rotational cyber workforce program in a manner that is consistent with the merit system principles under section 2301(b) of title 5, United States Code.
(B) TERM.—Except as provided in subparagraph (C), and notwithstanding section 3341(b) of title 5, United States Code, a detail to a rotational cyber workforce position shall be for a period of not less than 180 days and not more than 1 year.
(C) EXTENSION.—The Chief Human Capital Officer of the agency to which an employee is detailed under the rotational cyber workforce program may extend the period of a detail described in subparagraph (B) for a period of 60 days unless the Chief Human Capital Officer of the employing agency of the employee objects to that extension.
(4) WRITTEN SERVICE AGREEMENTS.—
(A) IN GENERAL.—The detail of an employee to a rotational cyber workforce position shall be contingent upon the employee entering into a written service agreement with the employing agency under which the employee is required to complete a period of employment with the employing agency following the conclusion of the detail that is equal in length to the period of the detail.
(B) OTHER AGREEMENTS AND OBLIGATIONS.—A written service agreement under subparagraph (A) shall not supersede or modify the terms or conditions of any other service agreement entered into by the employee under any other authority or relieve the obligations between the employee and the employing agency under such a service agreement. Nothing in this subparagraph prevents an employing agency from terminating a service agreement entered into under any other authority under the terms of such agreement or as required by law or regulation.

SEC. 4355. REPORTING BY GAO.

Not later than the end of the third fiscal year after the fiscal year in which the operation plan under section 4354(a) is issued, the Comptroller General of the United States shall submit to Congress a report assessing the operation and effectiveness of the rotational cyber workforce program, which shall address, at a minimum—
(1) the extent to which agencies have participated in the rotational cyber workforce program, including whether the head of each such participating agency has—
(A) identified positions within the agency that are rotational cyber workforce positions;
(B) had employees from other participating agencies serve in positions described in subparagraph (A); and
(C) had employees of the agency request to serve in rotational cyber workforce positions under the rotational cyber workforce program in participating agencies, including a description of how many such requests were approved; and
(2) the experiences of employees serving in rotational cyber workforce positions under the rotational cyber workforce program, including an assessment of—
(A) the period of service;
(B) the positions (including grade level and occupational series or work level) held by employees before completing service in a rotational cyber workforce position under the rotational cyber workforce program;
(C) the extent to which each employee who completed service in a rotational cyber workforce position under the rotational cyber workforce program achieved a higher skill level, or attained a skill level in a different area, with respect to information technology, cybersecurity, or other cyber-related functions; and
(D) the extent to which service in rotational cyber workforce positions has affected intra-agency and interagency integration and coordination of cyber practices, functions, and personnel management.

SEC. 4356. SUNSET.

Effective 5 years after the date of enactment of this Act, this subtitle is repealed.

TITLE IV—OTHER MATTERS

Subtitle A—Ensuring Security of Unmanned Aircraft Systems

SEC. 4401. SHORT TITLE.

This subtitle may be cited as the ''American Security Drone Act of 2021''.

SEC. 4402. DEFINITIONS.

In this subtitle:
(1) COVERED FOREIGN ENTITY.—The term ''covered foreign entity'' means an entity included on a list developed and maintained by the Federal Acquisition Security Council. This list will include entities in the following categories:
(A) An entity included on the Consolidated Screening List.

(B) Any entity that is subject to extrajudicial direction from a foreign government, as determined by the Secretary of Homeland Security.

(C) Any entity the Secretary of Homeland Security, in coordination with the Director of National Intelligence and the Secretary of Defense, determines poses a national security risk.

(D) Any entity domiciled in the People's Republic of China or subject to influence or control by the Government of the People's Republic of China or the Communist Party of the People's Republic of China, as determined by the Secretary of Homeland Security.

(E) Any subsidiary or affiliate of an entity described in subparagraphs (A) through (D).

(2) COVERED UNMANNED AIRCRAFT SYSTEM.—The term ''covered unmanned aircraft system'' has the meaning given the term ''unmanned aircraft system'' in section 44801 of title 49, United States Code.

SEC. 4403. PROHIBITION ON PROCUREMENT OF COVERED UNMANNED AIRCRAFT SYSTEMS FROM COVERED FOREIGN ENTITIES.

(a) IN GENERAL.—Except as provided under subsections (b) though (f), the head of an executive agency may not procure any covered unmanned aircraft system that are manufactured or assembled by a covered foreign entity, which includes associated elements (consisting of communication links and the components that control the unmanned aircraft) that are required for the operator to operate safely and efficiently in the national airspace system. The Federal Acquisition Security Council, in coordination with the Secretary of Transportation, shall develop and update a list of associated elements.

(b) EXEMPTION.—The Secretary of Homeland Security, the Secretary of Defense, and the Attorney General are exempt from the restriction under subsection (a) if the operation or procurement—

(1) is for the sole purposes of research, evaluation, training, testing, or analysis for—

(A) electronic warfare;

(B) information warfare operations;

(C) development of UAS or counter-UAS technology;

(D) counterterrorism or counterintelligence activities; or

(E) Federal criminal or national security investigations, including forensic examinations; and

(2) is required in the national interest of the United States.

(c) FEDERAL AVIATION ADMINISTRATION CENTER OF EXCELLENCE FOR UNMANNED AIRCRAFT SYSTEMS EXEMPTION.—The Secretary of Transportation, in consultation with the Secretary of Homeland Security, is exempt from the restriction under subsection (a) if the operation or procurement is for the sole purposes of research, evaluation, training, testing, or analysis for the Federal Aviation Administration's Alliance for System Safety of UAS through Research Excellence (ASSURE) Center of Excellence (COE) for Unmanned Aircraft Systems.

(d) NATIONAL TRANSPORTATION SAFETY BOARD EXEMPTION.—The National Transportation Safety Board (NTSB), in consultation with the Secretary of Homeland Security, is exempt from the restriction under subsection (a) if the operation or procurement is necessary for the sole purpose of conducting safety investigations.

(e) NATIONAL OCEANIC ATMOSPHERIC ADMINISTRATION EXEMPTION.—The Administrator of the National Oceanic Atmospheric Administration (NOAA), in consultation with the Secretary of Homeland Security, is exempt from the restriction under subsection (a) if the operation or procurement is necessary for the sole purpose of marine or atmospheric science or management.

(f) WAIVER.—The head of an executive agency may waive the prohibition under subsection (a) on a case-by-case basis—

(1) with the approval of the Secretary of Homeland Security or the Secretary of Defense; and

(2) upon notification to Congress.

SEC. 4404. PROHIBITION ON OPERATION OF COVERED UNMANNED AIRCRAFT SYSTEMS FROM COVERED FOREIGN ENTITIES.

(a) PROHIBITION.—

(1) IN GENERAL.—Beginning on the date that is 2 years after the date of the enactment of this Act, no Federal department or agency may operate a covered unmanned aircraft system manufactured or assembled by a covered foreign entity.

(2) APPLICABILITY TO CONTRACTED SERVICES.—The prohibition under paragraph (1) applies to any covered unmanned aircraft systems that are being used by any executive agency through the method of contracting for the services of covered unmanned aircraft systems.

(b) EXEMPTION.—The Secretary of Homeland Security, the Secretary of Defense, and the Attorney General are exempt from the restriction under subsection (a) if the operation or procurement—

(1) is for the sole purposes of research, evaluation, training, testing, or analysis for—

(A) electronic warfare;

(B) information warfare operations;

(C) development of UAS or counter-UAS technology;

(D) counterterrorism or counterintelligence activities; or

(E) Federal criminal or national security investigations, including forensic examinations; and

(2) is required in the national interest of the United States.

(c) FEDERAL AVIATION ADMINISTRATION CENTER OF EXCELLENCE FOR UNMANNED AIRCRAFT SYSTEMS EXEMPTION.—The Secretary of Transportation, in consultation with the Secretary of Homeland Security, is exempt from the restriction under subsection (a) if the operation or procurement is for the sole purposes of research, evaluation, training, testing, or analysis for the Federal Aviation Administration's Alliance for System Safety of UAE through Research Excellence (ASSURE) Center of Excellence (COE) for Unmanned Aircraft Systems.

(d) NATIONAL TRANSPORTATION SAFETY BOARD EXEMPTION.—The National Transportation Safety Board (NTSB), in consultation with the Secretary of Homeland Security, is exempt from the restriction under subsection (a) if the operation or procurement is necessary for the sole purpose of conducting safety investigations.

(e) NATIONAL OCEANIC ATMOSPHERIC ADMINISTRATION EXEMPTION.—The Administrator of the National Oceanic Atmospheric Administration (NOAA), in consultation with the Secretary of Homeland Security, is exempt from the restriction under subsection (a) if the operation or procurement is necessary for the sole purpose of marine or atmospheric science or management.

(f) WAIVER.—The head of an executive agency may waive the prohibition under subsection (a) on a case-by-case basis—

(1) with the approval of the Secretary of Homeland Security or the Secretary of Defense; and

(2) upon notification to Congress.

(g) REGULATIONS AND GUIDANCE.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall prescribe regulations or guidance to implement this section.

SEC. 4405. PROHIBITION ON USE OF FEDERAL FUNDS FOR PURCHASES AND OPERATION OF COVERED UNMANNED AIRCRAFT SYSTEMS FROM COVERED FOREIGN ENTITIES.

(a) IN GENERAL.—Beginning on the date that is 2 years after the date of the enactment of this Act, except as provided in subsection (b), no Federal funds awarded through a contract, grant, or cooperative agreement, or otherwise made available may be used—

(1) to purchase a covered unmanned aircraft system, or a system to counter unmanned aircraft systems, that is manufactured or assembled by a covered foreign entity; or

(2) in connection with the operation of such a drone or unmanned aircraft system.

(b) EXEMPTION.—A Federal department or agency is exempt from the restriction under subsection (a) if—

(1) the contract, grant, or cooperative agreement was awarded prior to the date of the enactment of this Act; or

(2) the operation or procurement is for the sole purposes of research, evaluation, training, testing, or analysis, as determined by the Secretary of Homeland Security, the Secretary of Defense, or the Attorney General, for—

(A) electronic warfare;

(B) information warfare operations;

(C) development of UAS or counter-UAS technology;

(D) counterterrorism or counterintelligence activities; or

(E) Federal criminal or national security investigations, including forensic examinations; or

(F) the safe integration of UAS in the national airspace (as determined in consultation with the Secretary of Transportation); and

(3) is required in the national interest of the United States.

(c) WAIVER.—The head of an executive agency may waive the prohibition under subsection (a) on a case-by-case basis—

(1) with the approval of the Secretary of Homeland Security or the Secretary of Defense; and

(2) upon notification to Congress.

(d) REGULATIONS.—Not later than 180 days after the date of the enactment of this Act, the Federal Acquisition Regulatory Council shall prescribe regulations or guidance, as necessary, to implement the requirements of this section pertaining to Federal contracts.

SEC. 4406. PROHIBITION ON USE OF GOVERNMENT-ISSUED PURCHASE CARDS TO PURCHASE COVERED UNMANNED AIRCRAFT SYSTEMS FROM COVERED FOREIGN ENTITIES.

Effective immediately, Government-issued Purchase Cards may not be used to procure any covered unmanned aircraft system from a covered foreign entity.

SEC. 4407. MANAGEMENT OF EXISTING INVENTORIES OF COVERED UNMANNED AIRCRAFT SYSTEMS FROM COVERED FOREIGN ENTITIES.

(a) IN GENERAL.—Effective immediately, all executive agencies must account for existing inventories of covered unmanned aircraft systems manufactured or assembled by a covered foreign entity in their personal property accounting systems, regardless of the original procurement cost, or the purpose of procurement due to the special monitoring and accounting measures necessary to track the items' capabilities.

(b) CLASSIFIED TRACKING.—Due to the sensitive nature of missions and operations conducted by the United States Government, inventory data related to covered unmanned aircraft systems manufactured or assembled by a covered foreign entity may be tracked at a classified level.

(c) EXCEPTIONS.—The Department of Defense and Department of Homeland Security may exclude from the full inventory process, covered unmanned aircraft systems that are deemed expendable due to mission risk such as recovery issues or that are one-time-use covered unmanned aircraft due to requirements and low cost.

SEC. 4408. COMPTROLLER GENERAL REPORT.

Not later than 275 days after the date of the enactment of this Act, the Comptroller General of the United States shall submit to Congress a report on the amount of commercial off-the-shelf drones and covered unmanned aircraft systems procured by Federal departments and agencies from covered foreign entities.

SEC. 4409. GOVERNMENT-WIDE POLICY FOR PROCUREMENT OF UNMANNED AIRCRAFT SYSTEMS.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of the Office of Management and Budget, in coordination with the Department of Homeland Security, Department of Transportation, the Department of Justice, and other Departments as determined by the Director of the Office of Management and Budget, and in consultation with the National Institute of Standards and Technology, shall establish a government-wide policy for the procurement of UAS—

(1) for non-Department of Defense and non-intelligence community operations; and

(2) through grants and cooperative agreements entered into with non-Federal entities.

(b) INFORMATION SECURITY.—The policy developed under subsection (a) shall include the following specifications, which to the extent practicable, shall be based on industry standards and technical guidance from the National Institute of Standards and Technology, to address the risks associated with processing, storing and transmitting Federal information in a UAS:

(1) Protections to ensure controlled access of UAS.

(2) Protecting software, firmware, and hardware by ensuring changes to UAS are properly managed, including by ensuring UAS can be updated using a secure, controlled, and configurable mechanism.

(3) Cryptographically securing sensitive collected, stored, and transmitted data, including proper handling of privacy data and other controlled unclassified information.

(4) Appropriate safeguards necessary to protect sensitive information, including during and after use of UAS.

(5) Appropriate data security to ensure that data is not transmitted to or stored in non-approved locations.

(6) The ability to opt out of the uploading, downloading, or transmitting of data that is not required by law or regulation and an ability to choose with whom and where information is shared when it is required.

(c) REQUIREMENT.—The policy developed under subsection (a) shall reflect an appropriate risk-based approach to information security related to use of UAS.

(d) REVISION OF ACQUISITION REGULATIONS.—Not later than 180 days after the date on which the policy required under subsection (a) is issued—

(1) the Federal Acquisition Regulatory Council shall revise the Federal Acquisition Regulation, as necessary, to implement the policy; and

(2) any Federal department or agency or other Federal entity not subject to, or not subject solely to, the Federal Acquisition Regulation shall revise applicable policy, guidance, or regulations, as necessary, to implement the policy.

(e) EXEMPTION.—In developing the policy required under subsection (a), the Director of the Office of Management and Budget shall incorporate an exemption to the policy for the following reasons:

(1) In the case of procurement for the purposes of training, testing, or analysis for—

(A) electronic warfare; or

(B) information warfare operations.

(2) In the case of researching UAS technology, including testing, evaluation, research, or development of technology to counter UAS.

(3) In the case of a head of the procuring department or agency determining, in writing, that no product that complies with the information security requirements described in subsection (b) is capable of fulfilling mission critical performance requirements, and such determination—

(A) may not be delegated below the level of the Deputy Secretary of the procuring department or agency;

(B) shall specify—

(i) the quantity of end items to which the waiver applies, the procurement value of which may not exceed $50,000 per waiver; and

(ii) the time period over which the waiver applies, which shall not exceed 3 years;

(C) shall be reported to the Office of Management and Budget following issuance of such a determination; and

(D) not later than 30 days after the date on which the determination is made, shall be provided to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives.

SEC. 4410. STUDY.

(a) INDEPENDENT STUDY.—Not later than 3 years after the date of the enactment of this Act, the Director of the Office of Management and Budget shall seek to enter into a contract with a federally funded research and development center under which the center will conduct a study of—

(1) the current and future unmanned aircraft system global and domestic market;

(2) the ability of the unmanned aircraft system domestic market to keep pace with technological advancements across the industry;

(3) the ability of domestically made unmanned aircraft systems to meet the network security and data protection requirements of the national security enterprise;

(4) the extent to which unmanned aircraft system component parts, such as the parts described in section 4403, are made domestically; and

(5) an assessment of the economic impact, including cost, of excluding the use of foreign-made UAS for use across the Federal Government.

(b) SUBMISSION TO OMB.—Upon completion of the study in subsection (a), the federally funded research and development center shall submit the study to the Director of the Office of Management and Budget.

(c) SUBMISSION TO CONGRESS.—Not later than 30 days after the date on which the Director of the Office of Management and Budget receives the study under subsection (b), the Director shall submit the study to—

(1) the Committee on Homeland Security and Governmental Affairs and the Select Committee on Intelligence of the Senate; and

(2) the Committee on Homeland Security and the Committee on Oversight and Reform and the Permanent Select Committee on Intelligence of the House of Representatives.

SEC. 4411. SUNSET.

Sections 4403, 4404, and 4405 shall cease to have effect on the date that is 5 years after the date of the enactment of this Act.

Subtitle B—No TikTok on Government Devices

SEC. 4431. SHORT TITLE.

This subtitle may be cited as the ''No TikTok on Government Devices Act''.

SEC. 4432. PROHIBITION ON THE USE OF TIKTOK.

(a) DEFINITIONS.—In this section—

(1) the term ''covered application'' means the social networking service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited;

(2) the term ''executive agency'' has the meaning given that term in section 133 of title 41, United States Code; and

(3) the term ''information technology'' has the meaning given that term in section 11101 of title 40, United States Code.

(b) PROHIBITION ON THE USE OF TIKTOK.—

(1) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Director of the Office of Management and Budget, in consultation with the Administrator of General Services, the Director of the Cybersecurity and Infrastructure Security Agency, the Director of National Intelligence, and the Secretary of Defense, and consistent with the information security requirements under subchapter II of chapter 35 of title 44, United States Code, shall develop standards and guidelines for executive agencies requiring the removal of any covered application from information technology.

(2) NATIONAL SECURITY AND RESEARCH EXCEPTIONS.—The standards and guidelines developed under paragraph (1) shall include—

(A) exceptions for law enforcement activities, national security interests and activities, and security researchers; and

(B) for any authorized use of a covered application under an exception, requirements for executive agencies to develop and document risk mitigation actions for such use.

Subtitle C—National Risk Management

SEC. 4461. SHORT TITLE.

This subtitle may be cited as the ''National Risk Management Act of 2021''.

SEC. 4462. NATIONAL RISK MANAGEMENT CYCLE.

(a) IN GENERAL.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended by adding at the end the following:

''SEC. 2218. NATIONAL RISK MANAGEMENT CYCLE.

''(a) NATIONAL CRITICAL FUNCTIONS DEFINED.—In this section, the term 'national critical functions' means the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

''(b) NATIONAL RISK MANAGEMENT CYCLE.—

''(1) RISK IDENTIFICATION AND ASSESSMENT.—

''(A) IN GENERAL.—The Secretary, acting through the Director, shall establish a recurring process by which to identify, assess, and prioritize risks to critical infrastructure, considering both cyber and physical threats, the associated likelihoods, vulnerabilities, and consequences, and the resources necessary to address them.

''(B) CONSULTATION.—In establishing the process required under subparagraph (A), the Secretary shall consult with, and request and collect information to support analysis from, Sector Risk Management Agencies, critical infrastructure owners and operators, the Assistant to the President for National Security Affairs, the Assistant to the President for Homeland Security, and the National Cyber Director.

''(C) PUBLICATION.—Not later than 180 days after the date of enactment of this section,

the Secretary shall publish in the Federal Register procedures for the process established under subparagraph (A), subject to any redactions the Secretary determines are necessary to protect classified or other sensitive information.

''(D) REPORT.—The Secretary shall submit to the President, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a report on the risks identified by the process established under subparagraph (A)—

''(i) not later than 1 year after the date of enactment of this section; and

''(ii) not later than 1 year after the date on which the Secretary submits a periodic evaluation described in section 9002(b)(2) of title XC of division H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116–283).

''(2) NATIONAL CRITICAL INFRASTRUCTURE RESILIENCE STRATEGY.—

''(A) IN GENERAL.—Not later than 1 year after the date on which the Secretary delivers each report required under paragraph (1), the President shall deliver to majority and minority leaders of the Senate, the Speaker and minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a national critical infrastructure resilience strategy designed to address the risks identified by the Secretary.

''(B) ELEMENTS.—Each strategy delivered under subparagraph (A) shall—

''(i) identify, assess, and prioritize areas of risk to critical infrastructure that would compromise or disrupt national critical functions impacting national security, economic security, or public health and safety;

''(ii) assess the implementation of the previous national critical infrastructure resilience strategy, as applicable;

''(iii) identify and outline current and proposed national-level actions, programs, and efforts to be taken to address the risks identified;

''(iv) identify the Federal departments or agencies responsible for leading each national-level action, program, or effort and the relevant critical infrastructure sectors for each; and

''(v) request any additional authorities necessary to successfully execute the strategy.

''(C) FORM.—Each strategy delivered under subparagraph (A) shall be unclassified, but may contain a classified annex.

''(3) CONGRESSIONAL BRIEFING.—Not later than 1 year after the date on which the President delivers the first strategy required under paragraph (2)(A), and every year thereafter, the Secretary, in coordination with Sector Risk Management Agencies, shall brief the appropriate congressional committees on—

''(A) the national risk management cycle activities undertaken pursuant to the strategy; and

''(B) the amounts and timeline for funding that the Secretary has determined would be necessary to address risks and successfully execute the full range of activities proposed by the strategy.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended by inserting after the item relating to section 2217 the following:

''Sec. 2218. National risk management cycle.''.

Subtitle D—Safeguarding American Innovation

SEC. 4491. SHORT TITLE.

This subtitle may be cited as the ''Safeguarding American Innovation Act''.

SEC. 4492. DEFINITIONS.

In this subtitle:

(1) FEDERAL SCIENCE AGENCY.—The term ''Federal science agency'' means any Federal department or agency to which more than $100,000,000 in basic and applied research and development funds were appropriated for the previous fiscal year.

(2) RESEARCH AND DEVELOPMENT.—

(A) IN GENERAL.—The term ''research and development'' means all research activities, both basic and applied, and all development activities.

(B) DEVELOPMENT.—The term ''development'' means experimental development.

(C) EXPERIMENTAL DEVELOPMENT.—The term ''experimental development'' means creative and systematic work, drawing upon knowledge gained from research and practical experience, which—

(i) is directed toward the production of new products or processes or improving existing products or processes; and

(ii) like research, will result in gaining additional knowledge.

(D) RESEARCH.—The term ''research''—

(i) means a systematic study directed toward fuller scientific knowledge or understanding of the subject studied; and

(ii) includes activities involving the training of individuals in research techniques if such activities—

(I) utilize the same facilities as other research and development activities; and

(II) are not included in the instruction function.

SEC. 4493. FEDERAL RESEARCH SECURITY COUNCIL.

(a) IN GENERAL.—Subtitle V of title 31, United States Code, is amended by adding at the end the following:

''CHAPTER 79—FEDERAL RESEARCH SECURITY COUNCIL

''§ 7901. Definitions

''In this chapter:

''(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means—

''(A) the Committee on Homeland Security and Governmental Affairs of the Senate;

''(B) the Committee on Commerce, Science, and Transportation of the Senate;

''(C) the Select Committee on Intelligence of the Senate;

''(D) the Committee on Foreign Relations of the Senate;

''(E) the Committee on Armed Services of the Senate;

''(F) the Committee on Health, Education, Labor, and Pensions of the Senate;

''(G) the Committee on Oversight and Reform of the House of Representatives;

''(H) the Committee on Homeland Security of the House of Representatives;

''(I) the Committee on Energy and Commerce of the House of Representatives;

''(J) the Permanent Select Committee on Intelligence of the House of Representatives;

''(K) the Committee on Foreign Affairs of the House of Representatives;

''(L) the Committee on Armed Services of the House of Representatives; and

''(M) the Committee on Education and Labor of the House of Representatives.

''(2) COUNCIL.—The term 'Council' means the Federal Research Security Council established under section 7902(a).

''(3) EXECUTIVE AGENCY.—The term 'Executive agency' has the meaning given that term in section 105 of title 5.

''(4) FEDERAL RESEARCH SECURITY RISK.—The term 'Federal research security risk' means the risk posed by malign state actors and other persons to the security and integrity of research and development conducted using research and development funds awarded by Executive agencies.

''(5) INSIDER.—The term 'insider' means any person with authorized access to any United States Government resource, including personnel, facilities, information, research, equipment, networks, or systems.

''(6) INSIDER THREAT.—The term 'insider threat' means the threat that an insider will use his or her authorized access (wittingly or unwittingly) to harm the national and economic security of the United States or negatively affect the integrity of a Federal agency's normal processes, including damaging the United States through espionage, sabotage, terrorism, unauthorized disclosure of national security information or nonpublic information, a destructive act (which may include physical harm to another in the workplace), or through the loss or degradation of departmental resources, capabilities, and functions.

''(7) RESEARCH AND DEVELOPMENT.—

''(A) IN GENERAL.—The term 'research and development' means all research activities, both basic and applied, and all development activities.

''(B) DEVELOPMENT.—The term 'development' means experimental development.

''(C) EXPERIMENTAL DEVELOPMENT.—The term 'experimental development' means creative and systematic work, drawing upon knowledge gained from research and practical experience, which—

''(i) is directed toward the production of new products or processes or improving existing products or processes; and

''(ii) like research, will result in gaining additional knowledge.

''(D) RESEARCH.—The term 'research'—

''(i) means a systematic study directed toward fuller scientific knowledge or understanding of the subject studied; and

''(ii) includes activities involving the training of individuals in research techniques if such activities—

''(I) utilize the same facilities as other research and development activities; and

''(II) are not included in the instruction function.

''(8) UNITED STATES RESEARCH COMMUNITY.—The term 'United States research community' means—

''(A) research and development centers of Executive agencies;

''(B) private research and development centers in the United States, including for profit and nonprofit research institutes;

''(C) research and development centers at institutions of higher education (as defined in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a)));

''(D) research and development centers of States, United States territories, Indian tribes, and municipalities;

''(E) government-owned, contractor-operated United States Government research and development centers; and

''(F) any person conducting federally funded research or receiving Federal research grant funding.

''§ 7902. Federal Research Security Council establishment and membership

''(a) ESTABLISHMENT.—There is established, in the Office of Management and Budget, a Federal Research Security Council, which

shall develop federally funded research and development grant making policy and management guidance to protect the national and economic security interests of the United States.

''(b) MEMBERSHIP.—

''(1) IN GENERAL.—The following agencies shall be represented on the Council:

''(A) The Office of Management and Budget.

''(B) The Office of Science and Technology Policy.

''(C) The Department of Defense.

''(D) The Department of Homeland Security.

''(E) The Office of the Director of National Intelligence.

''(F) The Department of Justice.

''(G) The Department of Energy.

''(H) The Department of Commerce.

''(I) The Department of Health and Human Services.

''(J) The Department of State.

''(K) The Department of Transportation.

''(L) The National Aeronautics and Space Administration.

''(M) The National Science Foundation.

''(N) The Department of Education.

''(O) The Small Business Administration.

''(P) The Council of Inspectors General on Integrity and Efficiency.

''(Q) Other Executive agencies, as determined by the Chairperson of the Council.

''(2) LEAD REPRESENTATIVES.—

''(A) DESIGNATION.—Not later than 45 days after the date of the enactment of the Safeguarding American Innovation Act, the head of each agency represented on the Council shall designate a representative of that agency as the lead representative of the agency on the Council.

''(B) FUNCTIONS.—The lead representative of an agency designated under subparagraph (A) shall ensure that appropriate personnel, including leadership and subject matter experts of the agency, are aware of the business of the Council.

''(c) CHAIRPERSON.—

''(1) DESIGNATION.—Not later than 45 days after the date of the enactment of the Safeguarding American Innovation Act, the Director of the Office of Management and Budget shall designate a senior level official from the Office of Management and Budget to serve as the Chairperson of the Council.

''(2) FUNCTIONS.—The Chairperson shall perform functions that include—

''(A) subject to subsection (d), developing a schedule for meetings of the Council;

''(B) designating Executive agencies to be represented on the Council under subsection (b)(1)(Q);

''(C) in consultation with the lead representative of each agency represented on the Council, developing a charter for the Council; and

''(D) not later than 7 days after completion of the charter, submitting the charter to the appropriate congressional committees.

''(3) LEAD SCIENCE ADVISOR.—The Director of the Office of Science and Technology Policy shall designate a senior level official to be the lead science advisor to the Council for purposes of this chapter.

''(4) LEAD SECURITY ADVISOR.—The Director of the National Counterintelligence and Security Center shall designate a senior level official from the National Counterintelligence and Security Center to be the lead security advisor to the Council for purposes of this chapter.

''(d) MEETINGS.—The Council shall meet not later than 60 days after the date of the enactment of the Safeguarding American Innovation Act and not less frequently than quarterly thereafter.

''§ 7903. Functions and authorities

''(a) DEFINITIONS.—In this section:

''(1) IMPLEMENTING.—The term 'implementing' means working with the relevant Federal agencies, through existing processes and procedures, to enable those agencies to put in place and enforce the measures described in this section.

''(2) UNIFORM APPLICATION PROCESS.—The term 'uniform application process' means a process employed by Federal science agencies to maximize the collection of information regarding applicants and applications, as determined by the Council.

''(b) IN GENERAL.—The Chairperson of the Council shall consider the missions and responsibilities of Council members in determining the lead agencies for Council functions. The Council shall perform the following functions:

''(1) Developing and implementing, across all Executive agencies that award research and development grants, awards, and contracts, a uniform application process for grants in accordance with subsection (c).

''(2) Developing and implementing policies and providing guidance to prevent malign foreign interference from unduly influencing the peer review process for federally funded research and development.

''(3) Identifying or developing criteria for sharing among Executive agencies and with law enforcement and other agencies, as appropriate, information regarding individuals who violate disclosure policies and other policies related to research security.

''(4) Identifying an appropriate Executive agency—

''(A) to accept and protect information submitted by Executive agencies and non-Federal entities based on the process established pursuant to paragraph (1); and

''(B) to facilitate the sharing of information received under subparagraph (A) to support, consistent with Federal law—

''(i) the oversight of federally funded research and development;

''(ii) criminal and civil investigations of misappropriated Federal funds, resources, and information; and

''(iii) counterintelligence investigations.

''(5) Identifying, as appropriate, Executive agencies to provide—

''(A) shared services, such as support for conducting Federal research security risk assessments, activities to mitigate such risks, and oversight and investigations with respect to grants awarded by Executive agencies; and

''(B) common contract solutions to support the verification of the identities of persons participating in federally funded research and development.

''(6) Identifying and issuing guidance, in accordance with subsection (e) and in coordination with the National Insider Threat Task Force established by Executive Order 13587 (50 U.S.C. 3161 note) for expanding the scope of Executive agency insider threat programs, including the safeguarding of research and development from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels and the distinct needs, missions, and systems of each such agency.

''(7) Identifying and issuing guidance for developing compliance and oversight programs for Executive agencies to ensure that research and development grant recipients accurately report conflicts of interest and conflicts of commitment in accordance with subsection (c)(1). Such programs shall include an assessment of—

''(A) a grantee's support from foreign sources and affiliations, appointments, or participation in talent programs with foreign funding institutions or laboratories; and

''(B) the impact of such support and affiliations, appointments, or participation in talent programs on United States national security and economic interests.

''(8) Providing guidance to Executive agencies regarding appropriate application of consequences for violations of disclosure requirements.

''(9) Developing and implementing a cross-agency policy and providing guidance related to the use of digital persistent identifiers for individual researchers supported by, or working on, any Federal research grant with the goal to enhance transparency and security, while reducing administrative burden for researchers and research institutions.

''(10) Engaging with the United States research community in conjunction with the National Science and Technology Council and the National Academies Science, Technology and Security Roundtable created under section 1746 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92; 42 U.S.C. 6601 note) in performing the functions described in paragraphs (1), (2), and (3) and with respect to issues relating to Federal research security risks.

''(11) Carrying out such other functions, consistent with Federal law, that are necessary to reduce Federal research security risks.

''(c) REQUIREMENTS FOR UNIFORM GRANT APPLICATION PROCESS.—In developing the uniform application process for Federal research and development grants required under subsection (b)(1), the Council shall—

''(1) ensure that the process—

''(A) requires principal investigators, co-principal investigators, and key personnel associated with the proposed Federal research or development grant project—

''(i) to disclose biographical information, all affiliations, including any foreign military, foreign government-related organizations, and foreign-funded institutions, and all current and pending support, including from foreign institutions, foreign governments, or foreign laboratories, and all support received from foreign sources; and

''(ii) to certify the accuracy of the required disclosures under penalty of perjury; and

''(B) uses a machine-readable application form to assist in identifying fraud and ensuring the eligibility of applicants;

''(2) design the process—

''(A) to reduce the administrative burden on persons applying for Federal research and development funding; and

''(B) to promote information sharing across the United States research community, while safeguarding sensitive information; and

''(3) complete the process not later than 1 year after the date of the enactment of the Safeguarding American Innovation Act.

''(d) REQUIREMENTS FOR INFORMATION SHARING CRITERIA.—In identifying or developing criteria and procedures for sharing information with respect to Federal research security risks under subsection (b)(3), the Council shall ensure that such criteria address, at a minimum—

''(1) the information to be shared;

''(2) the circumstances under which sharing is mandated or voluntary;

''(3) the circumstances under which it is appropriate for an Executive agency to rely on information made available through such sharing in exercising the responsibilities and authorities of the agency under applicable laws relating to the award of grants;

''(4) the procedures for protecting intellectual capital that may be present in such information; and

''(5) appropriate privacy protections for persons involved in Federal research and development.

''(e) REQUIREMENTS FOR INSIDER THREAT PROGRAM GUIDANCE.—In identifying or developing guidance with respect to insider threat programs under subsection (b)(6), the Council shall ensure that such guidance provides for, at a minimum—

''(1) such programs—

''(A) to deter, detect, and mitigate insider threats; and

''(B) to leverage counterintelligence, security, information assurance, and other relevant functions and resources to identify and counter insider threats; and

''(2) the development of an integrated capability to monitor and audit information for the detection and mitigation of insider threats, including through—

''(A) monitoring user activity on computer networks controlled by Executive agencies;

''(B) providing employees of Executive agencies with awareness training with respect to insider threats and the responsibilities of employees to report such threats;

''(C) gathering information for a centralized analysis, reporting, and response capability; and

''(D) information sharing to aid in tracking the risk individuals may pose while moving across programs and affiliations;

''(3) the development and implementation of policies and procedures under which the insider threat program of an Executive agency accesses, shares, and integrates information and data derived from offices within the agency and shares insider threat information with the executive agency research sponsors;

''(4) the designation of senior officials with authority to provide management, accountability, and oversight of the insider threat program of an Executive agency and to make resource recommendations to the appropriate officials; and

''(5) such additional guidance as is necessary to reflect the distinct needs, missions, and systems of each Executive agency.

''(f) ISSUANCE OF WARNINGS RELATING TO RISKS AND VULNERABILITIES IN INTERNATIONAL SCIENTIFIC COOPERATION.—

''(1) IN GENERAL.—The Council, in conjunction with the lead security advisor designated under section 7902(c)(4), shall establish a process for informing members of the United States research community and the public, through the issuance of warnings described in paragraph (2), of potential risks and vulnerabilities in international scientific cooperation that may undermine the integrity and security of the United States research community or place at risk any federally funded research and development.

''(2) CONTENT.—A warning described in this paragraph shall include, to the extent the Council considers appropriate, a description of—

''(A) activities by the national government, local governments, research institutions, or universities of a foreign country—

''(i) to exploit, interfere, or undermine research and development by the United States research community; or

''(ii) to misappropriate scientific knowledge resulting from federally funded research and development;

''(B) efforts by strategic competitors to exploit the research enterprise of a foreign country that may place at risk—

''(i) the science and technology of that foreign country; or

''(ii) federally funded research and development; and

''(C) practices within the research enterprise of a foreign country that do not adhere to the United States scientific values of openness, transparency, reciprocity, integrity, and merit-based competition.

''(g) EXCLUSION ORDERS.—To reduce Federal research security risk, the Interagency Suspension and Debarment Committee shall provide quarterly reports to the Director of the Office of Management and Budget and the Director of the Office of Science and Technology Policy that detail—

''(1) the number of ongoing investigations by Council Members related to Federal research security that may result, or have resulted, in agency pre-notice letters, suspensions, proposed debarments, and debarments;

''(2) Federal agencies' performance and compliance with interagency suspensions and debarments;

''(3) efforts by the Interagency Suspension and Debarment Committee to mitigate Federal research security risk;

''(4) proposals for developing a unified Federal policy on suspensions and debarments; and

''(5) other current suspension and debarment related issues.

''(h) SAVINGS PROVISION.—Nothing in this section may be construed—

''(1) to alter or diminish the authority of any Federal agency; or

''(2) to alter any procedural requirements or remedies that were in place before the date of the enactment of the Safeguarding American Innovation Act.

''§ 7904. Annual report

''Not later than November 15 of each year, the Chairperson of the Council shall submit a report to the appropriate congressional committees that describes the activities of the Council during the preceding fiscal year.

''§ 7905. Requirements for Executive agencies

''(a) IN GENERAL.—The head of each Executive agency on the Council shall be responsible for—

''(1) assessing Federal research security risks posed by persons participating in federally funded research and development;

''(2) avoiding or mitigating such risks, as appropriate and consistent with the standards, guidelines, requirements, and practices identified by the Council under section 7903(b);

''(3) prioritizing Federal research security risk assessments conducted under paragraph (1) based on the applicability and relevance of the research and development to the national security and economic competitiveness of the United States; and

''(4) ensuring that initiatives impacting Federally funded research grant making policy and management to protect the national and economic security interests of the United States are integrated with the activities of the Council.

''(b) INCLUSIONS.—The responsibility of the head of an Executive agency for assessing Federal research security risk described in subsection (a) includes—

''(1) developing an overall Federal research security risk management strategy and implementation plan and policies and processes to guide and govern Federal research security risk management activities by the Executive agency;

''(2) integrating Federal research security risk management practices throughout the lifecycle of the grant programs of the Executive agency;

''(3) sharing relevant information with other Executive agencies, as determined appropriate by the Council in a manner consistent with section 7903; and

''(4) reporting on the effectiveness of the Federal research security risk management strategy of the Executive agency consistent with guidance issued by the Office of Management and Budget and the Council.''.

(b) CLERICAL AMENDMENT.—The table of chapters at the beginning of title 31, United States Code, is amended by inserting after the item relating to chapter 77 the following:

SEC. 4494. FEDERAL GRANT APPLICATION FRAUD.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by adding at the end the following:

''§ 1041. Federal grant application fraud

''(a) DEFINITIONS.—In this section:

''(1) FEDERAL AGENCY.—The term 'Federal agency' has the meaning given the term 'agency' in section 551 of title 5, United States Code.

''(2) FEDERAL GRANT.—The term 'Federal grant'—

''(A) means a grant awarded by a Federal agency;

''(B) includes a subgrant awarded by a non-Federal entity to carry out a Federal grant program; and

''(C) does not include—

''(i) direct United States Government cash assistance to an individual;

''(ii) a subsidy;

''(iii) a loan;

''(iv) a loan guarantee; or

''(v) insurance.

''(3) FEDERAL GRANT APPLICATION.—The term 'Federal grant application' means an application for a Federal grant.

''(4) FOREIGN COMPENSATION.—The term 'foreign compensation' means a title, monetary compensation, access to a laboratory or other resource, or other benefit received from—

''(A) a foreign government;

''(B) a foreign government institution; or

''(C) a foreign public enterprise.

''(5) FOREIGN GOVERNMENT.—The term 'foreign government' includes a person acting or purporting to act on behalf of—

''(A) a faction, party, department, agency, bureau, subnational administrative entity, or military of a foreign country; or

''(B) a foreign government or a person purporting to act as a foreign government, regardless of whether the United States recognizes the government.

''(6) FOREIGN GOVERNMENT INSTITUTION.—The term 'foreign government institution' means a foreign entity owned by, subject to the control of, or subject to regulation by a foreign government.

''(7) FOREIGN PUBLIC ENTERPRISE.—The term 'foreign public enterprise' means an enterprise over which a foreign government directly or indirectly exercises a dominant influence.

''(8) LAW ENFORCEMENT AGENCY.—The term 'law enforcement agency'—

''(A) means a Federal, State, local, or Tribal law enforcement agency; and

''(B) includes—

''(i) the Office of Inspector General of an establishment (as defined in section 12 of the Inspector General Act of 1978 (5 U.S.C. App.)) or a designated Federal entity (as defined in section 8G(a) of the Inspector General Act of 1978 (5 U.S.C. App.)); and

''(ii) the Office of Inspector General, or similar office, of a State or unit of local government.

''(9) OUTSIDE COMPENSATION.—The term 'outside compensation' means any compensation, resource, or support (regardless of monetary value) made available to the applicant in support of, or related to, any research endeavor, including a title, research grant, cooperative agreement, contract, institutional award, access to a laboratory, or other resource, including materials, travel compensation, or work incentives.

''(b) PROHIBITION.—It shall be unlawful for any individual to knowingly—

''(1) prepare or submit a Federal grant application that fails to disclose the receipt of any outside compensation, including foreign compensation, by the individual;

''(2) forge, counterfeit, or otherwise falsify a document for the purpose of obtaining a Federal grant; or

''(3) prepare, submit, or assist in the preparation or submission of a Federal grant application or document in connection with a Federal grant application that—

''(A) contains a false statement;

''(B) contains a material misrepresentation;

''(C) has no basis in law or fact; or

''(D) fails to disclose a material fact.

''(c) EXCEPTION.—Subsection (b) does not apply to an activity—

''(1) carried out in connection with a lawfully authorized investigative, protective, or intelligence activity of—

''(A) a law enforcement agency; or

''(B) a Federal intelligence agency; or

''(2) authorized under chapter 224.

''(d) PENALTY.—Any individual who violates subsection (b)—

''(1) shall be fined in accordance with this title, imprisoned for not more than 5 years, or both; and

''(2) shall be prohibited from receiving a Federal grant during the 5-year period beginning on the date on which a sentence is imposed on the individual under paragraph (1).''.

(b) CLERICAL AMENDMENT.—The analysis for chapter 47 of title 18, United States Code, is amended by adding at the end the following:

''1041. Federal grant application fraud.''.

SEC. 4495. RESTRICTING THE ACQUISITION OF EMERGING TECHNOLOGIES BY CERTAIN ALIENS.

(a) GROUNDS OF INADMISSIBILITY.—The Secretary of State may determine that an alien is inadmissible if the Secretary determines such alien is seeking to enter the United States to knowingly acquire sensitive or emerging technologies to undermine national security interests of the United States by benefitting an adversarial foreign government's security or strategic capabilities.

(b) RELEVANT FACTORS.—To determine if an alien is inadmissible under subsection (a), the Secretary of State shall—

(1) take account of information and analyses relevant to implementing subsection (a) from the Office of the Director of National Intelligence, the Department of Health and Human Services, the Department of Defense, the Department of Homeland Security, the Department of Energy, the Department of Commerce, and other appropriate Federal agencies;

(2) take account of the continual expert assessments of evolving sensitive or emerging technologies that foreign adversaries are targeting;

(3) take account of relevant information concerning the foreign person's employment or collaboration, to the extent known, with—

(A) foreign military and security related organizations that are adversarial to the United States;

(B) foreign institutions involved in the theft of United States research;

(C) entities involved in export control violations or the theft of intellectual property;

(D) a government that seeks to undermine the integrity and security of the United States research community; or

(E) other associations or collaborations that pose a national security threat based on intelligence assessments; and

(4) weigh the proportionality of risks and the factors listed in paragraphs (1) through (3).

(c) REPORTING REQUIREMENT.—Not later than 180 days after the date of the enactment of this Act, and semi-annually thereafter until the sunset date set forth in subsection (e), the Secretary of State, in coordination with the Director of National Intelligence, the Director of the Office of Science and Technology Policy, the Secretary of Homeland Security, the Secretary of Defense, the Secretary of Energy, the Secretary of Commerce, and the heads of other appropriate Federal agencies, shall submit a report to the Committee on the Judiciary of the Senate, the Committee on Foreign Relations of the Senate, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on the Judiciary of the House of Representatives, the Committee on Foreign Affairs of the House of Representatives, and the Committee on Oversight and Reform of the House of Representatives that identifies—

(1) any criteria, if relevant used to describe the aliens to which the grounds of inadmissibility described in subsection (a) may apply;

(2) the number of individuals determined to be inadmissible under subsection (a), including the nationality of each such individual and the reasons for each determination of inadmissibility; and

(3) the number of days from the date of the consular interview until a final decision is issued for each application for a visa considered under this section, listed by applicants' country of citizenship and relevant consulate.

(d) CLASSIFICATION OF REPORT.—Each report required under subsection (c) shall be submitted, to the extent practicable, in an unclassified form, but may be accompanied by a classified annex.

(e) SUNSET.—This section shall cease to be effective on the date that is 2 years after the date of the enactment of this Act.

SEC. 4496. MACHINE READABLE VISA DOCUMENTS.

(a) MACHINE-READABLE DOCUMENTS.—Not later than 1 year after the date of the enactment of this Act, the Secretary of State shall—

(1) use a machine-readable visa application form; and

(2) make available documents submitted in support of a visa application in a machine readable format to assist in—

(A) identifying fraud;

(B) conducting lawful law enforcement activities; and

(C) determining the eligibility of applicants for a visa under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).

(b) WAIVER.—The Secretary of State may waive the requirement under subsection (a) by providing to Congress, not later than 30 days before such waiver takes effect—

(1) a detailed explanation for why the waiver is being issued; and

(2) a timeframe for the implementation of the requirement under subsection (a).

(c) REPORT.—Not later than 45 days after date of the enactment of this Act, the Secretary of State shall submit a report to the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Commerce, Science, and Transportation of the Senate, the Select Committee on Intelligence of the Senate, the Committee on Foreign Relations of the Senate; the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, the Committee on Energy and Commerce of the House of Representatives, the Permanent Select Committee on Intelligence of the House of Representatives, and the Committee on Foreign Affairs of the House of Representatives that—

(1) describes how supplementary documents provided by a visa applicant in support of a visa application are stored and shared by the Department of State with authorized Federal agencies;

(2) identifies the sections of a visa application that are machine-readable and the sections that are not machine-readable;

(3) provides cost estimates, including personnel costs and a cost-benefit analysis for adopting different technologies, including optical character recognition, for—

(A) making every element of a visa application, and documents submitted in support of a visa application, machine-readable; and

(B) ensuring that such system—

(i) protects personally-identifiable information; and

(ii) permits the sharing of visa information with Federal agencies in accordance with existing law; and

(4) includes an estimated timeline for completing the implementation of subsection (a).

SEC. 4497. CERTIFICATIONS REGARDING ACCESS TO EXPORT CONTROLLED TECHNOLOGY IN EDUCATIONAL AND CULTURAL EXCHANGE PROGRAMS.

Section 102(b)(5) of the Mutual Educational and Cultural Exchange Act of 1961 (22 U.S.C. 2452(b)(5)) is amended to read as follows:

''(5) promoting and supporting medical, scientific, cultural, and educational research and development by developing exchange programs for foreign researchers and scientists, while protecting technologies regulated by export control laws important to the national security and economic interests of the United States, by requiring—

''(A) the sponsor to certify to the Department of State that the sponsor, after reviewing all regulations related to the Export Controls Act of 2018 (50 U.S.C. 4811 et seq.) and the Arms Export Control Act (22 U.S.C. 2751 et seq.), has determined that—

''(i) a license is not required from the Department of Commerce or the Department of State to release such technology or technical data to the exchange visitor; or

''(ii)(I) a license is required from the Department of Commerce or the Department of State to release such technology or technical data to the exchange visitor; and

''(II) the sponsor will prevent access to the controlled technology or technical data by the exchange visitor until the sponsor—

''(aa) has received the required license or other authorization to release it to the visitor; and

''(bb) has provided a copy of such license or authorization to the Department of State; and

''(B) if the sponsor maintains export controlled technology or technical data, the sponsor to submit to the Department of State the sponsor's plan to prevent unauthorized export or transfer of any controlled items, materials, information, or technology at the sponsor organization or entities associated with a sponsor's administration of the exchange visitor program.''.

SEC. 4498. PRIVACY AND CONFIDENTIALITY.

Nothing in this subtitle may be construed as affecting the rights and requirements provided in section 552a of title 5, United States Code (commonly known as the ''Privacy Act of 1974'') or subchapter III of chapter 35 of title 44, United States Code (commonly known as the ''Confidential Information Protection and Statistical Efficiency Act of 2018'').

SA 4293. Mr. PORTMAN submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military